CTIA
The Wireless Association®

GSMA

Global IMEI Database

June 19th 2014

CTIA's Role in the Industry

CTIA The Wireless Association®

GSMA

CTIA-The Wireless Association® (www.ctia.org) is an international organization representing the wireless communications industry and is headquartered in Washington DC. CTIA advocates on behalf of its members at all levels of government, including all 50 States and industry, globally.

The association also coordinates the industry's voluntary best practices and initiatives, and sponsors the industry's leading wireless tradeshows.

CTIA Members

- Wireless Carriers, Network Operators
- Device Manufacturers
- Network manufacturers
- Platform providers
- Application providers
- Content providers

GSMA's Role in the Industry

CTIA
The Wireless Association®

GSMA

The GSMA represents the interests of mobile operators worldwide. Spanning more than 220 countries, the GSMA unites nearly 800 of the world's mobile operators with 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organizations in industry sectors such as financial services, healthcare, media, transport and utilities. The GSMA also produces industry-leading events such as Mobile World Congress and Mobile Asia Expo.

IMEI Global Database

- On April 10, 2012, CTIA – The Wireless Association® (“CTIA”), in coordination with the Federal Communications Commission and the Major City Police Chiefs, announced a voluntary commitment by CTIA and participating wireless companies to take certain actions to help law enforcement deter smartphone theft and protect personal data.
- Implement databases to prevent reactivation of stolen smartphones. Wireless providers implement and deploy database solutions, using unique smartphone identifying numbers, designed to prevent smartphones reported by their customers as stolen from being activated and/or provided service on their own networks.
- Database online in the US as of November 2013

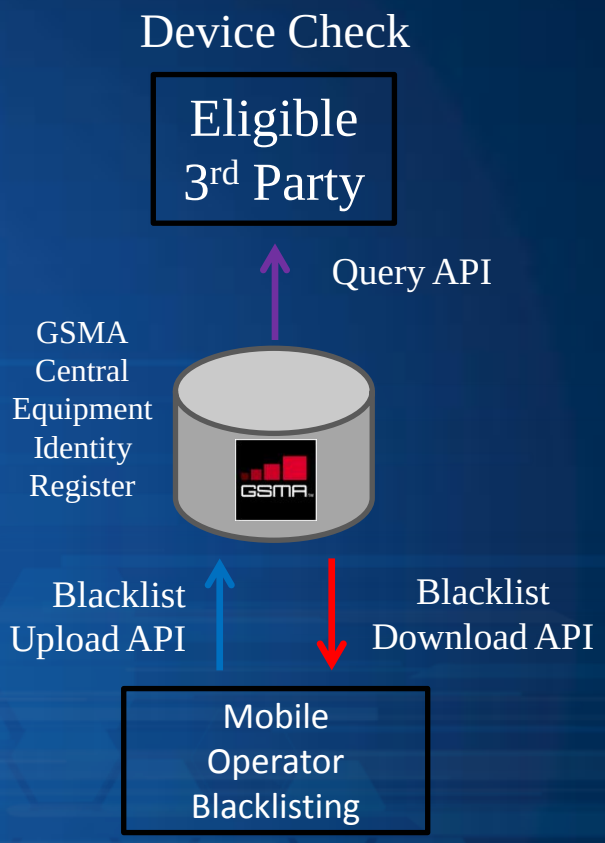
IMEI – International Mobile Equipment Identifier, CTIA Administers IMEI Assignment for the US

Device Check

- Blacklisting/Device Check
  - What is it?
  - Recent Developments
  - Blacklist Ecosystem
  - Device Check Use Cases
  - IMEI Blacklisting Service Overview
  - Benefits
  - How to participate – Operator/Industry

What is Blacklisting?

- GSMA global Registry of Blacklisted devices
- Data exchange of blocked devices between operators
- Allows devices to be blocked not only on home networks but also adjacent networks
- Allows insurers, dealers and recyclers to detect stolen devices
- Government agencies use for checking
- 42 countries participating*
- Operational for over 10 years
- Reduce significant financial losses from theft and fraud



* As of June 2014

CTIA
The Wireless Association®

Recent Developments

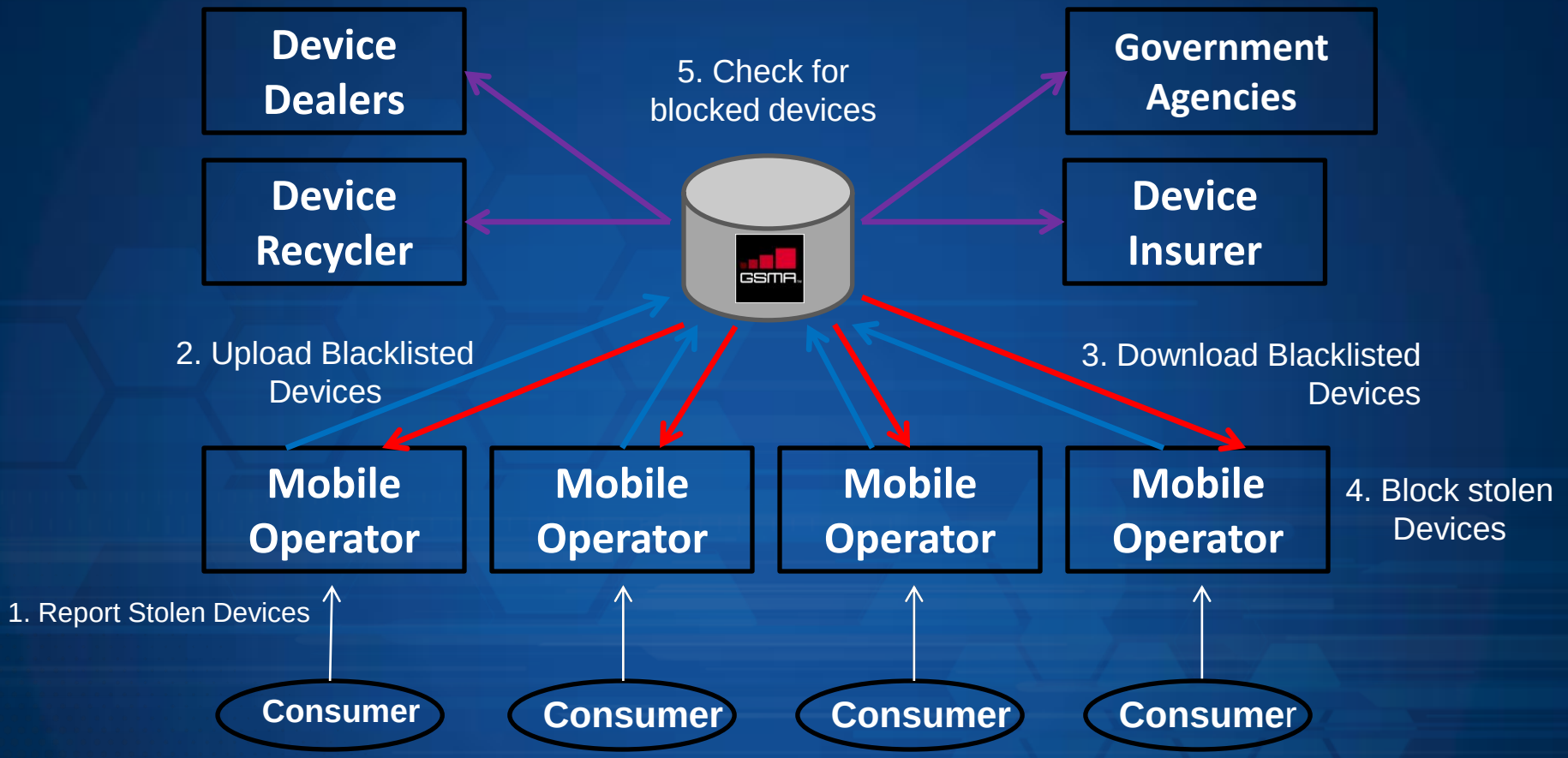
GSMA

- Device Check launched Oct 2012
- AT&T, T-Mobile, Verizon and Sprint - Blacklist Registry Nov 2013, USA/Canadian operators now connected
- Tri agreement signed for French Police/Gendarmerie/Border controls Dec 2013
- NYPD connected to 3rd party access Jan 2014
- Significant roll-out underway throughout USA

Blacklist Ecosystem

CTIA
The Wireless Association®

GSMA



Device Check Use cases

CTIA The Wireless Association®

GSMA

- **Second hand devices have substantial financial value and are therefore a target for theft and fraud**
- **Consequence of device crime:**
  - Operator loss of device subsidy investment
  - Device theft can lead to churn
  - Recyclers are target for illegal device laundering
  - Consumer pays out of pocket for replacement device
  - Insurance premiums go up
  - Excessive claims deter insurance underwriters
- **Conclusion:**
  - It is in the best interest for Consumers, Operators, Device Recyclers, and Government organisations to deter device crime by exchanging information

IMEI Blacklist Service Overview

CTIA The Wireless Association®

GSMA

- List of all device IMEIs reported as lost or stolen
- Synchronised with participating Operator networks regularly
- Used to block lost or stolen devices from accessing the network
- Free to member Operators

TAC	Marketing Name	IMEIs On Black List	IMEIs On Grey List	Manufacturer Name
990004	Apple iPhone 4S (A1387)	0	0	Apple Inc.
	BlackBerry RFX101LW	0	0	Research in Motion, Ltd.
	CN50NR	0	0	Intermec Technologies
	Kyocera Torque	0	0	Kyocera Communications Inc.
	Samsung Galaxy S Camera	0	0	Samsung Telecom America
		Total: 0	**Total: 0**	
990003	Apple iPad (A1460)	78	0	Apple Inc.
	Apple iPad mini (A1455)	27	0	Apple Inc.
	Apple iPhone 4S (A1387)	0	0	Apple Inc.

Registration Process

- Maintain an Equipment Identity Register (EIR)
- Request CNO (Connected Network Operator) status in the IMEI website
- Receive connectivity credentials
- Synchronise with GSMA IMEI Blacklist daily

Benefits

Operators

- Allows sharing of device blacklisting data globally
- Enables blocking of stolen devices on participating operator networks
- Support for law enforcement protection of consumers
- Support recycling industry in anti laundering activities
- Supports insurance industry in fraudulent claim prevention

Benefits

CTIA The Wireless Association®

GSMA

Device Recyclers

- Aids in preventing handling stolen/lost devices
- Protects business financially
- Instils comfort in marketplace

Insurance Companies

- Help detect fraudulent claims
- Reduce financial loss
- Promotes underwriting confidence

Benefits

CTIA The Wireless Association®

GSMA

Government

- Police identify stolen handset on the street
- Customs identify stolen devices at boarders and authentication of model prior to importing/exporting

Consumers

- Carry out stolen handset checks before buying second hand
- Facilitates proof of purchase for warranty purposes

IMEI Database in the Press

- **Results:** Stolen phone database is working
- ***Some i-Phones bought on Craig's List can't be activated***
- http://www.wzzm13.com/story/news/local/lakeshore/2014/04/08/stolen-phones-sprint-burglaries/7492009/
- **Phones stolen from Sprint stores are now worthless**
- Phil Dawson, WZZM, *April 8, 2014*

Also:

- *Reported declines in thefts in Washington DC and San Francisco*

CTIA
The Wireless Association®

Smartphone Anti-Theft Voluntary Commitment

April 15, 2014 – CTIA and participating wireless companies announced the "Smartphone Anti-Theft Voluntary Commitment,"

New models of smartphones after July 2015 will offer, at no cost to consumers, a baseline anti-theft tool that is preloaded or downloadable on wireless smartphones that provides the capability to:

1. Remote wipe the authorized user's data (i.e., erase personal info that is added after purchase such as contacts, photos, emails, etc.) that is on the smartphone in the event it is lost or stolen.
2. Render the smartphone inoperable to an unauthorized user (e.g., locking the smartphone so it cannot be used without a password or PIN), except in accordance with FCC rules for 911 emergency communications, and if available, emergency numbers programmed by the authorized user (e.g., "phone home").
3. Prevent reactivation without authorized user's permission (including unauthorized factory reset attempts) to the extent technologically feasible (e.g., locking the smartphone as in 2 above).
4. Reverse the inoperability if the smartphone is recovered by the authorized user and restore user data on the smartphone to the extent feasible (e.g., restored from the cloud).

CTIA
The Wireless Association®

Thank you !

John A. Marinho
CTIA - The Wireless Association
1400 16th Street NW, Suite 600
Washington DC 20036
jmarinho@ctia.org
Mobile: 202-440-0844
Fixed: 202-736-3680